CHARACTERISTIC POLYNOMIALS AND FIXED SPACES OF SEMISIMPLE ELEMENTS

ROBERT GURALNICK AND GUNTER MALLE

Dedicated to Len Scott

Abstract. Answering a question of Frank Calegari, we extend some of our earlier results on dimension of fixed point spaces of elements in irreducible linear groups. We consider characteristic polynomials rather than just fixed spaces.

1. Introduction

In [10], the authors answered a question of Peter Neumann and proved that if G is a nontrivial irreducible subgroup of $\mathrm{GL}_n(k) = \mathrm{GL}(V)$ with k a field, then there exists an element $g \in G$ with $\dim C_V(g) \le (1/3)\dim V$ (where $C_V(g)$ denotes the fixed space of g acting on V). The example $G = \mathrm{SO}_3(k)$ with k not of characteristic 2 shows that $1/3$ is best possible.

Frank Calegari asked if one could find $g \in G$ such that the characteristic polynomial of g acting on V was of the form $(T-1)^e f(T)$ where $f(1) \neq 0$ and $e < n/2$. Calegari and Gee [2] are interested in the irreducibility of the Galois representations associated to self-dual cohomological automorphic forms for GL_n, especially for small n. This result is easily seen to be true for finite G (or more generally compact G) in characteristic 0 by the orthogonality relations (see [12, Section 3] for this simple proof). For finite groups (or more generally for algebraic groups or if the characteristic is positive), the question reduces to finding a semisimple element $g \in G$ with $\dim C_V(g) < n/2$ (recall an element in a linear group is semisimple if it is diagonalizable over the algebraic closure — for a finite group, this is equivalent to saying that $\mathrm{char}\, k$ does not divide the order of the element).

The authors in [10, Thm. 1.3] proved a conjecture of Peter Neumann from 1966 about the minimum dimension of fixed spaces. In particular, if G is finite and the characteristic does not divide $|G|$, this gives:

Theorem 1.1. *Let k be a field of characteristic $p \ge 0$ and G a nontrivial finite subgroup of $\mathrm{GL}_n(k) = \mathrm{GL}(V)$ with p not dividing $|G|$. If V is an irreducible kG-module, then there exists a semisimple element $g \in G$ with $\dim C_V(g) \le (1/3)\dim V$.*

We note that this result depends upon the classification of finite simple groups. However, the result had previously been unknown even for solvable groups.

The conclusion of the theorem no longer holds in non-coprime characteristic. The simplest example is to take $G = A.C$ the semidirect product of an elementary abelian group

Date: December 21, 2011.
2010 *Mathematics Subject Classification.* Primary 20C20.
The first author was partially supported by DMS 1001962. We thank Frank Calegari for his questions and comments.

A of order 8 with the cyclic group of order 7 acting faithfully. Then G has an irreducible 7-dimensional representation over any field of characteristic not 2. In particular, in characteristic 7, we see that every nontrivial semisimple element has a 3-dimensional fixed space. More generally, if $p = 2^a - 1$ is a Mersenne prime, let $G = A.C$ with A elementary abelian of order $p + 1 = 2^a$ and C of order p acting faithfully on A. Then G has an irreducible representation of dimension p in characteristic p and every nontrivial semisimple element has a fixed space of dimension $(p - 1)/2$. Moreover, taking direct products of this group with itself and the corresponding tensor product of representations, one gets examples of arbitrarily large dimension.

Even in characteristic 0, the Example 6.5 in [10] shows that one can do no better than $(1/9) \dim V$ no matter how large the dimension of V. In this note, we will prove Calegari's inequality and show that one can do better under various circumstances.

If we consider connected algebraic groups, we can obtain similar results that do not depend upon the classification of finite simple groups. Since a compact real Lie group has only semisimple elements and since the minimum value of $\dim C_V(g)$ is attained on a nonempty open subset of G, we also obtain:

Theorem 1.2. *Let $G \neq 1$ be a connected compact real Lie subgroup of $\mathrm{GL}_n(\mathbb{C}) = \mathrm{GL}(V)$. Assume that $C_V(G) = 0$. Then the average dimension (with respect to Haar measure) of $C_V(g)$ is at most $(1/3) \dim V$.*

Let $\epsilon > 0$. It was shown in [9, Thm. 6] that if G is compact and connected and V is irreducible, then in fact the average dimension of $C_V(g)$ is less than $\epsilon \dim V$ as long as $\dim V$ is sufficiently large.

We have a similar result for Zariski dense subgroups of connected algebraic groups.

Theorem 1.3. *Let $G \neq 1$ be a subgroup of $\mathrm{GL}_n(k) = \mathrm{GL}(V)$ with k an algebraically closed field and $\mathrm{char}\, k = p \geq 0$. Assume that V is completely reducible, $C_V(G) = 0$ and the Zariski closure of G is connected. Then the set of semisimple $g \in G$ with $\dim C_V(g) \leq (1/3) \dim V$ is open and Zariski dense in G.*

An easy consequence of Theorem 1.3 is:

Corollary 1.4. *Let G be an irreducible subgroup of $\mathrm{GL}_n(k) = \mathrm{GL}(V)$ with $\mathrm{char}\, k = p \geq 0$. Assume that G is infinite. Then there exists a semisimple $g \in G$ such that $\dim C_V(g) \leq (1/3) \dim V$.*

Thus, we are reduced to considering finite groups. For the general case, we can show:

Theorem 1.5. *Let $1 \neq G \leq \mathrm{GL}_n(k) = \mathrm{GL}(V)$ with $\mathrm{char}\, k = p \geq 0$. Assume that G acts irreducibly on V.*

(a) *There exists a semisimple $g \in G$ with $\dim C_V(g) < (1/2) \dim V$.*
(b) *If $p > n + 2$ or $p = 0$, then there exists a semisimple $g \in G$ with $\dim C_V(g) \leq (1/3) \dim V$.*
(c) *If p does not divide n, then there exists a semisimple $g \in G$ with $\dim C_V(g) \leq (3/8) \dim V$.*
(d) *If n is prime and 2 is a multiplicative generator modulo n, then there exists a semisimple $g \in G$ with $\dim C_V(g) \leq (1/3) \dim V$.*

In particular, this shows that if $n \leq 5$, there exists a semisimple element $g \in G$ with $\dim C_V(g) \leq 1$. If n is prime, one can prove even stronger results:

Theorem 1.6. *Let G be a finite irreducible subgroup of $\mathrm{GL}_n(k)$ with n an odd prime. Assume that $\mathrm{char}\, k = p > 2n-3$ (or $p = 0$). There exists a semisimple element $x \in G$ with all eigenspaces of dimension at most 1.*

The paper is organized as follows. In the next section, we deal with algebraic groups and deduce the various results on algebraic and infinite groups. We then consider various generation results about finite simple groups. In particular, in Section 3 we prove the following results that may be of independent interest:

Theorem 1.7. *Let G be a finite nonabelian simple group and p be a prime. Then unless $(G, p) = (\mathfrak{A}_5, 5)$, there exist p'-elements $x, y, z \in G$ with $xyz = 1$ such that $G = \langle x, y \rangle$.*

Theorem 1.8. *Let G be a finite nonabelian simple group and p be a prime. Then there exist a pair of conjugate p'-elements that generate G.*

Note that an immediate consequence of Theorem 1.7 and Scott's Lemma [18] is:

Corollary 1.9. *Let G be a finite nonabelian simple subgroup of $\mathrm{GL}_n(k) = \mathrm{GL}(V)$. Assume that $C_V(G) = C_{V^*}(G) = 0$. If $G = \mathfrak{A}_5$ and $\mathrm{char}\, k = 5$, assume further that V has no trivial composition factors. Then there exists a semisimple element $g \in G$ with $\dim C_V(g) \leq (1/3) \dim V$.*

It is shown [10, Thm. 6.1] that in fact if $\epsilon > 0$, G is a nonabelian finite simple group and V is an irreducible $\mathbb{C}G$-module, then there exists $g \in G$ with $\dim C_V(g) < \epsilon \dim V$ as long as $\dim V$ is sufficiently large (or equivalently $|G|$ is sufficiently large). This should be true for any algebraically closed field.

In Section 4, we consider finite groups and prove Theorem 1.5(a)–(c). We then consider representations of prime dimension, complete the proof of Theorem 1.5 and prove Theorem 1.6. In the final section, we give some examples relating to the divisibility of characteristic polynomials of representations (a question asked by Calegari [2]).

2. Infinite Groups

In this section we prove Theorems 1.2, 1.3 and Corollary 1.4. These results do not require the classification of finite simple groups.

We first prove Theorem 1.3. Let k be an algebraically closed field of characteristic $p \geq 0$. Let G be a subgroup of $\mathrm{GL}_n(k) = \mathrm{GL}(V)$. We assume that G has no trivial composition factors on V and that Γ, the Zariski closure of G is connected.

Our assumption is that G (equivalently Γ) acts completely reducibly on V. Thus, Γ is reductive. Note that for any $e \geq 0$, $\{g \in \Gamma \mid \dim C_V(g) \leq e\}$ is an open subvariety of Γ. Moreover, the set of semisimple elements of Γ is also open.

Let S be a rational irreducible $k\Gamma$-module. If follows by [7, Thm. 3.3] that the set of pairs of semisimple elements in Γ which generate an irreducible subgroup on S is a nontrivial open subvariety of Γ^2. Thus, the set of pairs of semisimple elements in Γ which have no fixed points on V and whose product is semisimple is also an open nonempty subvariety of Γ^2. Thus, this set intersects G^2 in a nonempty open subset of G^2. Choose $x, y \in G$ such that $\langle x, y \rangle$ has no fixed points on V with x, y and xy semisimple.

By Scott's Lemma [18], $\dim C_V(x) + \dim C_V(y) + \dim C_V(xy) \leq \dim V$ and so some semisimple element $g \in G$ satisfies $\dim C_V(g) \leq (1/3)\dim V$. This shows that the set of semisimple elements of Γ with $\dim C_V(g) \leq (1/3)\dim V$ is an open dense subvariety of Γ. In particular, this set must intersect G whence Theorem 1.3 holds. Theorem 1.2 now follows immediately.

We now prove Corollary 1.4. Arguing as in [10, Thm. 5.8], it suffices to work over an algebraically closed field. Let Γ be the Zariski closure of G and Γ° the connected component of the identity in Γ. Note that $\Gamma^\circ \neq 1$ as G is infinite. Since V is irreducible for G, hence for Γ, Γ° acts completely reducibly without fixed points on V. By Theorem 1.3, the set of semisimple $g \in \Gamma^\circ$ with $\dim C_V(g) \leq (1/3)\dim V$ contains a dense open subset of Γ° and therefore intersects $G \cap \Gamma^\circ$ non-trivially, as required.

We close this section by showing that often one can do even better in the case of algebraic groups. There is a version of the following theorem for semisimple groups as well.

Theorem 2.1. *Let G be a simple simply connected algebraic group of rank r at least 2 over an algebraically closed field k. Let V be a completely reducible rational kG-module with $C_V(G) = 0$. Let $g \in G$ be a regular semisimple element and assume that g^3 is not central (the latter can only fail if $G = \mathrm{SL}_3$). Then:*

(a) *$\dim C_V(g) \leq (1/3)\dim V$, and*

(b) *if g^2 is also regular, then every eigenspace of g has dimension at most $(1/3)\dim V$.*

Proof. Let C be the conjugacy class of g. We first prove (a). Let X be the variety of triples of elements all in C with product 1. By [11, Thms. 6.11, 6.15], this is an irreducible variety (of dimension $2\dim G - 3r$) and the set of triples in X which generate a subgroup H such that each irreducible submodule of V remains irreducible for H (and non-isomorphic irreducibles remain non-isomorphic) is a dense open subvariety of X. Now (a) follows by Scott's Lemma.

If g^2 is regular semisimple, we consider the variety

$$Y = \{(x, y, z) \in C \times C \times C^{-2} \mid xyz = 1\}.$$

Precisely as above, we see that the subset of Y consisting of triples so that the subgroup they generate has the same collection of irreducibles as G is dense. Apply Scott's Lemma to the elements $(\lambda^{-1}x, \lambda^{-1}y, \lambda^2 z)$ to conclude that the λ-eigenspace of at least one of them has dimension at most $(1/3)\dim V$. □

Note that we do not need to assume that V is completely reducible in the previous result. The proof goes through verbatim as long as we assume that $C_V(G) = C_{V^*}(G) = 0$.

3. Generation results

The purpose of this section is the proof of the following generation results:

Theorem 3.1. *Let G be a finite non-abelian simple group, p a prime. Then we have:*

(a) *G is generated by two conjugate p'-elements, and*

(b) *G is generated by three p'-elements x, y, z with $xyz = 1$ unless $(G, p) = (\mathfrak{A}_5, 5)$.*

Note that $(\mathfrak{A}_5, 5)$ is a true exception to the conclusion of Theorem 3.1(b) since the largest element order of $\mathfrak{A}_5$ prime to 5 is 3, and the triangle groups $G(l,m,n)$ with $l,m,n \leq 3$ are solvable.

In [10, Thm. 1.1] we showed that any finite non-abelian simple group G is generated by a certain triple of conjugate elements with product 1. Thus the remaining task is to prove (a) and (b) for primes p dividing the common order of these elements. This will be shown in the subsequent propositions.

Proposition 3.2. *Theorem 3.1 holds for sporadic groups and the Tits group.*

Proof. For G a sporadic simple group both parts follow from [11, Table 4], where we exhibited a second generating systems (x,y,z) for G with product 1, with $x \sim y$ and the orders of x,y,z prime to those from [10]. □

Proposition 3.3. *Theorem 3.1 holds for alternating groups.*

Proof. For $G = \mathfrak{A}_n$ an alternating group, with $n \geq 11$ odd, we produced in [10, Lemma 4.2] a generating system (x_1, y_1, z_1) of $n-2$-cycles with product 1. In [5, Cor. 17] there is given a generating system (x_2, y_2, z_2) with x_2, y_2 squares of an $n-1$-cycle and $o(z_2) = n$. For $n \geq 12$ even, we gave a generating triple of $n-3$-cycles in [10, Lemma 4.3], while [5, Cor. 14] gives a generating system with x_2, y_2 both $n-1$-cycles and $o(z_2) = n/2$. This gives the claim unless $p = 3$ divides n. In the latter case, by [1, Cor. 2.2] for $n > 12$ there exists two $n-5$-cycles with product of type $(n-2)(2)$, and these generate a transitive group since otherwise, the three elements would be in $\mathfrak{S}_{n-2}$ with the first two being in $\mathfrak{A}_{n-2}$. The $n-5$ cycle guarantees the group generated is primitive and [20, Thm. 13.8] implies that they generate a 6-transitive group. The result now follows by [20, Thm. 51.1]. The alternating group $\mathfrak{A}_{12}$ has a generating triple consisting of elements of order 11.

For $n = 5,6,7,8,9,10$ we gave generating triples of orders 5,5,7,7,7,7 respectively in [10, Lemma 4.4]. For $n = 6,7,8,9,10$ direct computation shows that there also exist generating triples of orders 4,5,15,15,15. Note that $\mathfrak{A}_5$ is generated by two 3-cycles (with product of order 5). □

Proposition 3.4. *Theorem 3.1 holds for exceptional simple groups of Lie type.*

Proof. For G of exceptional Lie type different from ${}^3D_4(q)$, we produced in [11, Thm. 2.2] a second generating system consisting of conjugate elements, while for ${}^3D_4(q)$ in [11, Prop. 2.3] we gave a generating triple containing two conjugate elements. Moreover, in all cases, the element orders in these triples are coprime to those from [10]. □

Finally assume that G is of classical Lie type. For $n \geq 2$, we let $\Phi_n^*(q)$ denote the largest divisor of $q^n - 1$ that is relatively prime to $q^m - 1$ for all $1 \leq m < n$.

Proposition 3.5. *Theorem 3.1 holds for* $\mathrm{L}_2(q)$*,* $q \geq 4$*.*

Proof. The groups $\mathrm{L}_2(q)$ with $q \in \{4,5,9\}$ are isomorphic to alternating groups, for which the claim follows from Proposition 3.3. The group $\mathrm{L}_2(7)$ has generating triples consisting of elements of order 7, respectively of order 4. For $q \geq 8$, $q \neq 9$, we gave in [10, Lemmas 3.14, 3.15] generating triples for $\mathrm{L}_2(q)$ of orders $(q-1)/d$, where $d = \gcd(2, q-1)$. Similarly, a direct calculation shows that there exist generating triples of order $(q+1)/d$, which proves the claim. □

Definition 3.6. Let's say that a pair (C, D) of conjugacy classes of a group G is *generating* if $G = \langle x, y\rangle$ for all $(x, y) \in C \times D$.

Note that by the result of Gow [6], if (C, D) is a generating pair for a finite group of Lie type consisting of classes of regular semisimple elements, then we find generators $(x, y) \in C \times D$ with product in any given (noncentral) semisimple conjugacy class, for example in C^{-1}.

Proposition 3.7. *Theorem 3.1 holds for the groups* $\mathrm{L}_n(q)$*,* $n \geq 3$*.*

Proof. Let $G = \mathrm{L}_n(q)$, $n \geq 3$. Note that we may assume that $(n, q) \neq (3, 2), (4, 2)$ as $\mathrm{L}_3(2) \cong \mathrm{L}_2(7)$ and $\mathrm{L}_4(2) \cong \mathfrak{A}_8$ were already handled above. In [10, Prop. 3.13] we showed that G is generated by a triple of elements of order $\Phi_n^*(q)$ when n is odd, respectively of order $\Phi_{n-1}^*(q)$ when n is even. For $n \neq 4$ and $(n, q) \neq (6, 2)$, we showed in [11, Prop. 3.1 and 3.5] that there also exist generating triples of elements of orders coprime to the former ones, of the type stated in Theorem 3.1. The group $\mathrm{L}_6(2)$ is generated by a triple of elements of order 7.

Now consider $G = \mathrm{SL}_4(q)$. Let C be a conjugacy class of regular semisimple elements of order $(q^4 - 1)/(q - 1)$. According to [10, Lemma 2.3], the only maximal subgroups of $\mathrm{SL}_4(q)$ which might contain an element $x \in C$ are the normalizer of $\Omega_4^-(q)$, of $\mathrm{Sp}_4(q)$ or of $\mathrm{GL}_2(q^2) \cap \mathrm{SL}_4(q)$. But in the first two of these groups the centralizer order of elements of order $q^2 + 1$ is not divisible by $(q^2 + 1)(q + 1)$ when $q > 3$. Thus, any $x \in C$ lies in a unique maximal subgroup of G. Let C_2 denote a class of regular semisimple elements in a maximal torus of order $(q^2 - 1)(q - 1)$ of $\mathrm{SL}_4(q)$. Then this does not intersect the normalizer of $\mathrm{GL}_2(q^2) \cap \mathrm{SL}_4(q)$, so (C_1, C_2) is a generating pair. By [6] there exist pairs with product in C_1^{-1}, which must generate. Now pass to the quotient of $\mathrm{SL}_4(q)$ by its center. The group $\mathrm{L}_4(3)$ has a generating triple with elements of order 5. □

Proposition 3.8. *Theorem 3.1 holds for the unitary groups* $\mathrm{U}_n(q)$*,* $n \geq 3$*,* $(n, q) \neq (4, 2)$*.*

Proof. Let $G = \mathrm{U}_n(q)$, $n \geq 3$. The case $n = 3$ was already treated in [11, Prop. 3.1]. In [10, Prop. 3.11 and 3.12] we showed that G is generated by a triple of elements of order $\Phi_{2n}^*(q)$ when n is odd, respectively of order $\Phi_{2n-2}^*(q)$ when n is even. For $n \geq 8$ we showed in [11, Prop. 3.6] that there also exist generating triples of elements of orders coprime to the former ones, of the form required in Theorem 3.1. For the remaining n we argue in $G = \mathrm{SU}_n(q)$ and then pass to the quotient by the center. For $n = 7$ let C_1 contain elements of type 6^+ and C_2 elements of type $5^- \oplus 2^+$, for $n = 5$ let C_1 contain elements of type 4^+ and C_2 elements of type $3^- \oplus 2^+$. Then any pair from $C_1 \times C_2$ generates an irreducible subgroup, and by [10, Thm. 2.2] that can't be proper, when $(n, q) \neq (5, 2)$. We conclude using [6]. The group $\mathrm{U}_5(2)$ has generating triples of elements of order 5.

If $n = 4$ or 6, the claim of Theorem 3.1(b) holds by [11, Prop. 3.6]. For Theorem 3.1(a), the group $\mathrm{U}_6(2)$ has a generating triple of elements of order 7. Else let's take C_1 a class of elements of order $\Phi_{2n-2}^*(q)$, C_2 a class of elements of order $\Phi_4^*(q)$ when $n = 4$, $\Phi_3^*(q)\Phi_6^*(q)$ when $n = 6$, and C_3 one of C_1, C_2. Then the arguments in the proof of [10, Prop. 3.12] go through, with even better estimates, since the number of characters not vanishing on both C_1 and C_2 is smaller, and the same for the number of maximal subgroups containing elements from both classes. It follows that there exist generating triples with product 1

in $C_1 \times C_1 \times C_2$ and in $C_1 \times C_2 \times C_2$. Since the orders in the two classes are relatively coprime, this gives the result. □

Proposition 3.9. *Theorem 3.1 holds for the orthogonal groups* $\mathrm{O}_{2n+1}(q)$*,* $n \geq 3$*.*

Proof. The group $G = \mathrm{O}_{2n+1}(q)$ possesses a generating triple of elements of order $\Phi_{2n}^*(q)$, by [10, Prop. 3.7 and 3.8]. For $n \geq 7$, we produced in [11, Prop. 7.9] a generating pair (C, D) of conjugacy classes containing regular semisimple elements of orders prime to $\Phi_{2n}^*(q)$. For $n = 4, 5, 6$, let C contain elements of type $(n-1)^- \oplus 1^-$, D elements of type $(n-2)^- \oplus 2^+$. Then the group generated by $(x, y) \in C \times D$ acts irreducibly or is contained in a $2n$-dimensional orthogonal group. By consideration of suitable Zsigmondy primes, the latter can possibly only occur when $q \leq 3$, which we exclude for the moment. Otherwise, an application of [11, Cor. 3.4] shows that (C, D) is a generating pair, and we conclude using [6]. The groups $\mathrm{O}_9(2) \cong \mathrm{S}_8(2)$, $\mathrm{O}_9(3)$, $\mathrm{O}_{11}(2) \cong \mathrm{S}_{10}(2)$, $\mathrm{O}_{11}(3)$, $\mathrm{O}_{13}(2) \cong \mathrm{S}_{12}(2)$, $\mathrm{O}_{13}(3)$, possess generating triples with elements of orders 7, 13, 31, 41, 31, 61 respectively, Finally, for $n = 3$, we argued in [11, Prop. 3.8] that conjugacy classes of regular semisimple elements of types 3^+, $2^- \oplus 1^+$ form a generating pair in $\mathrm{O}_7(q)$ for $q \geq 5$, and we produced generating triples of orders 7, 13 and 17 for $\mathrm{O}_7(2) \cong \mathrm{S}_6(2)$, $\mathrm{O}_7(3)$, $\mathrm{O}_7(4)$ respectively. □

Proposition 3.10. *Theorem 3.1 holds for the symplectic groups* $\mathrm{S}_{2n}(q)$*,* $n \geq 2$*,* $(n, q) \neq (2, 2)$*.*

Proof. Note that we may assume that q is odd when $n \geq 3$ by the result of Proposition 3.9. The group $G = \mathrm{S}_{2n}(q)$ possesses a generating triple of elements of order $\Phi_{2n}^*(q)$, resp. order 5 when $(n, q) = (2, 3)$, by [10, Prop. 3.8]. For $n \geq 3$, $(n, q) \neq (4, 3)$, we found in [11, Prop. 7.8] a generating pair (C, D) of conjugacy classes containing regular semisimple elements of orders prime to $\Phi_{2n}^*(q)$, and we may conclude as usual. The group $\mathrm{S}_8(3)$ has a generating triple with elements of order 13.

For $\mathrm{S}_4(q)$ with $q \geq 3$, the claim was already proved in [11, Prop. 3.1]. □

Proposition 3.11. *Theorem 3.1 holds for the orthogonal groups* $\mathrm{O}_{2n}^+(q)$*,* $n \geq 4$*.*

Proof. Let $G = \mathrm{O}_{2n}^+(q)$, $n \geq 4$. In [10, Prop. 3.10] we showed that G is generated by a triple of elements of order dividing $\Phi_{2n-2}^*(q)(q+1)$. For $n \neq 4$ we showed in [11, Prop. 3.10] that there also exist generating pairs of conjugate regular semisimple elements of orders coprime to the former ones, and we may conclude as before.

For the $n = 4$ we may assume that $q \geq 3$, since for $\mathrm{O}_8^+(2)$ there exist generating triples of elements of order 9, and also of elements of order 7, by [10, Prop. 3.10] and [11, Prop. 3.10]. Let C_1 contain regular semisimple elements of order $(q^2+1)/d$, with $d = \gcd(2, q-1)$, in a maximal torus T of order $(q^2+1)^2/d^2$, and C_2 the image of C_1 under triality. Let $(x, y) \in C_1 \times C_2$. Then $H := \langle x, y \rangle$ contains T up to conjugation. By [16, Table I] the only maximal subgroup of $\mathrm{O}_8^+(q)$ with this property is $M = (\mathrm{O}_4^-(q) \times \mathrm{O}_4^-(q)).2^2$. According to [6] there are (x, y) with product of order a Zsigmondy prime divisor of q^2+q+1, and hence not contained in M. This gives a triple as in Theorem 3.1(b).

We now show Theorem 3.1(a) for $n = 4$ and $q \geq 3$. Let C_1 be a conjugacy class of elements of order $\Phi_6^*(q)$. Let C_2 be a conjugacy class of regular semisimple elements of order $(q^4-1)/4$ (or q^4-1 if q is even) having precisely two non-trivial invariant subspaces. Let C_3 be either C_1 or C_2. Arguing as in [10, Prop. 3.10], one gets a lower bound for the

number of triples $(x, y, z) \in C_1 \times C_2 \times C_3$ with product 1 (the bound is actually much better than in [10] since there will be many fewer characters not vanishing on C_1 and C_2). Similarly, one gets an upper bound for the number of non-generating such triples (again the bound is much better than that given in [10] since there are many fewer maximal subgroups — for example, it is clear the group generated is irreducible). It follows that two elements of C_1 or C_2 will generate. Since the orders of the elements in C_1 and C_2 are relatively prime, the result follows. □

Proposition 3.12. *Theorem 3.1 holds for the groups orthogonal $\mathrm{O}_{2n}^-(q)$, $n \geq 4$.*

Proof. The group $G = \mathrm{O}_{2n}^-(q)$ possesses a generating triple of elements of order $\Phi_{2n}^*(q)$, by [10, Prop. 3.6]. For $(n, q) \notin \{(4, 2), (4, 4), (5, 2), (6, 2)\}$, we produced in [11, Prop. 7.10] a generating pair (C, D) of conjugacy classes of G containing regular semisimple elements of orders prime to $\Phi_{2n}^*(q)$. Now by [6] there exist triples in $C \times C \times D$, for example. Direct computation shows that the groups $\mathrm{O}_8^-(2)$, $\mathrm{O}_8^-(4)$, $\mathrm{O}_{10}^-(2)$, $\mathrm{O}_{12}^-(2)$ possess generating triples with elements of orders 7, 13, 17, 31 respectively, which are again prime to $\Phi_{2n}^*(q)$. □

4. Finite Groups

Here, we prove Theorem 1.5(a)–(c). By Corollary 1.4 it suffices to consider finite groups.

Fix a field k of characteristic $\mathrm{char}\, k = p$. By Theorem 1.1, we may assume that $p > 0$. Assume that $1 \neq G \leq \mathrm{GL}_n(k) = \mathrm{GL}(V)$ is irreducible on V. By extending scalars, we can reduce to the case that k is algebraically closed (V would at worst be a direct sum of Galois conjugates of a given irreducible module).

Let N be a minimal normal subgroup of G. Thus, N acts completely reducibly on V and without fixed points. We break up the argument depending upon the structure of N.

Lemma 4.1. *If $|N|$ is odd, then N is an r-group for some odd prime $r \neq p$ and there exists a p'-element $g \in N$ with $\dim C_V(g) < (1/r) \dim V \leq (1/3) \dim V$.*

Proof. Since $|N|$ is odd, N is solvable and since it is a minimal normal subgroup, it must be an r-group with $r \neq p$. Now apply [12, Cor. 1.3]. □

Lemma 4.2. *If N is an elementary abelian 2-group, then $p \neq 2$ and*
(a) *there exists an involution $g \in N$ with $\dim C_V(g) < (1/2) \dim V$;*
(b) *if p does not divide $\dim V$, then there exists a p'-element $g \in G$ with $\dim C_V(g) \leq (1/3) \dim V$.*

Proof. Clearly, $p \neq 2$. By [12, Cor. 1.3], there exists $g \in N$ with $\dim C_V(g) < (1/2) \dim V$.

So we may assume that p does not divide $\dim V$. If N is central, then any $1 \neq g \in N$ satisfies $C_V(g) = 0$ and there is nothing to prove. Otherwise, $V = \bigoplus V_i$ where the V_i are the distinct N-eigenspaces. Since V is irreducible, G permutes the V_i transitively. By [4, Thm. 1], there exists $x \in G$ of prime power order r^a having no fixed points on the set of V_i. Since p does not divide $\dim V$, $r \neq p$. If r is odd, then every orbit of x has size at least 3 whence $\dim C_V(x) \leq (1/3) \dim V$. So we may assume that $r = 2$. It follows as in the proof of [10, Thm. 5.8] that the average dimension of the fixed point spaces of elements in the coset xN is at most $(1/4) \dim V$. Since every element in xN is a 2-element, the result follows. □

The remaining case is when N is a direct product of $t \geq 1$ isomorphic copies of a nonabelian simple group L. Let W be an irreducible kN-submodule of V. By reordering, we may write $W = U_1 \otimes \cdots \otimes U_t$ where each U_i is an irreducible kL-module with $U_i \cong k$ if and only if $i > m$ for some $m > 1$. First we note that the proof of [10, Cor. 5.7] gives:

Lemma 4.3. *Let L be a simple group of Lie type over a finite field of characteristic p and let $E = L \times \cdots \times L$. Let k be an algebraically closed field of characteristic p, V a completely reducible kE-module with $C_V(E) = 0$. Then there exists a semisimple element $x \in E$ with* $\dim C_V(x) \leq (1/3) \dim V$.

Actually, the proof in [10] does not work if $L \cong \mathrm{L}_2(5)$ with $p = 5$, or $L \cong \mathrm{L}_2(7)$ with $p = 7$. A more complicated proof can be given in these cases to show that the result is still true. The result also follows easily if $L \neq \mathrm{L}_2(q)$ using Theorem 2.1.

Lemma 4.4. *Let L be a nonabelian finite simple group and let $E = L \times \cdots \times L$ (t copies). Let k be an algebraically closed field of characteristic p, $V = U_1 \otimes \cdots \otimes U_t$ a nontrivial irreducible kE-module with* $\dim U_i = 3$ *for some i. There exists a p'-element $x \in E$ (independent of V) such that all eigenspaces of x have dimension at most* $(1/3) \dim V$.

Proof. First assume that $t = 1$, so $\dim V = 3$. By inspection, we can choose x of odd prime order with distinct eigenvalues (indeed unless $p = 3$, we can take x of order 3).

Suppose that $t > 1$. Let y be the element of E with all coordinates equal to the x chosen above. Since x has all eigenspaces of dimension at most $(1/3) \dim U_i$ on U_i, the same is true on V. $\square$

Lemma 4.5. *Let L be a finite group with $L = \langle x, y \rangle$ and let $E = L \times \cdots \times L$. Let k be an algebraically closed field of characteristic p, $V = U_1 \otimes \cdots \otimes U_t$ a nontrivial irreducible kE-module with* $\dim U_i \geq 4$ *for some U_i. Let G be a diagonal copy of L in E. Let x_1, y_1 and z_1 be elements of G with each coordinate x, y or $z = (xy)^{-1}$ respectively. Then* $\dim C_V(x_1) + \dim C_V(y_1) + \dim C_V(z_1) \leq (9/8) \dim V$. *In particular,*

$$\min\{\dim C_V(x_1), \dim C_V(y_1), \dim C_V(z_1)\} \leq (3/8) \dim V.$$

Proof. The assumption that some U_i has dimension at least 4 gives that $\dim C_V(G) \leq (1/16) \dim V$. Indeed, assume that $\dim U_1 \geq 4$. Then $C_V(G) \cong \mathrm{Hom}_G(U_1^*, U_2 \otimes \cdots \otimes U_t)$. Since $\dim U_1 \geq 4$,

$$\dim C_V(G) \leq (1/4) \dim(U_2 \otimes \cdots \otimes U_t) \leq (1/16) \dim V.$$

Similarly, $\dim C_{V^*}(G) \leq (1/16) \dim V$. By Scott's Lemma [18]

$$\begin{aligned} \dim C_V(x_1) + &\dim C_V(y_1) + \dim C_V(z_1) \\ &\leq \dim V + \dim C_V(G) + \dim C_{V^*}(G) \leq (9/8) \dim V. \end{aligned}$$

The result follows. $\square$

Corollary 4.6. *Let G be a finite group, k an algebraically closed field of characteristic p and V a faithful irreducible kG-module. Let $E = L \times \cdots \times L$ be a minimal normal subgroup of G with L a nonabelian simple group. Then there exists a p'-element $x \in E$ with* $\dim C_V(x) \leq (3/8) \dim V$.

Proof. If L is of Lie type in characteristic p, the result follows by Lemma 4.3. So assume that this is not the case.

Let W be any irreducible kE-submodule of V. Then $W = U_1 \otimes \cdots \otimes U_t$ where each U_i is an irreducible kL-module.

If $\dim U_i = 2$, then $p = 2$ and $L \cong \mathrm{SL}_2(2^f)$ is of Lie type in characteristic 2, whence the result by Lemma 4.3.

If $\dim U_i = 3$ for some i, then this will be the case for every irreducible kE-submodule (since any such is a twist of W) and Lemma 4.4 applies.

In the remaining case, $\dim U_i > 3$ for every nontrivial U_i (and similarly for every twist of W). By Theorem 1.7, we can choose p'-elements $x, y, z \in L$ which generate L and have product 1 aside from $(L, p) = (\mathfrak{A}_5, 5)$. Note that $\mathfrak{A}_5 \cong \mathrm{L}_2(5)$, so the latter is of Lie type in defining characteristic, a case we already dealt with (alternatively, it would follow that each nontrivial U_i has dimension 5 and so if x is an element of E with each coordinate of order 3, $\dim C_W(x) \leq (9/25) \dim V < (3/8) \dim W$). It follows by Lemma 4.5 that there exists a p'-element $g \in E$ with $\dim C_V(g) \leq (3/8) \dim V$. □

We can now prove the first three parts of Theorem 1.5.

Proof of Theorem 1.5. Parts (a) and (c) follow from Lemmas 4.1, 4.2 and Corollary 4.6.

Now assume that $p > \dim V + 2$. By Lemma 4.1, we may assume that G has no odd order non-trivial normal subgroups. If $O_2(G) \neq 1$, Lemma 4.2 applies since p does not divide $\dim V$. So we may assume that $F(G) = 1$. Let $N = L \times \cdots \times L$ be a minimal normal subgroup of G with L a nonabelian simple group. By [8, Thm. B], it follows that one of the following holds:

(1) p does not divide $|N|$;
(2) L is a finite group of Lie type in characteristic p; or
(3) $p = 11$, $N = J_1$ and $\dim V = 7$.

Thus by [10, Cor. 5.7] there exists $x \in N$ with $\dim C_V(x) \leq (1/3) \dim V$. If x is a p'-element, we are done. So we may assume that p divides the order of x (and so $|N|$).

If $N = J_1$, $p = 11$ and $\dim V = 7$, an element g of order 19 satisfies $\dim C_V(g) = 1 < (1/3) \dim V$. If L has Lie type, then Lemma 4.3 yields a semisimple element $g \in N$ with $\dim C_V(g) \leq (1/3) \dim V$. This completes the proof of (b). □

5. Prime Degree

Recall that a group is called quasi-simple if G is perfect and $G/Z(G)$ is a nonabelian simple group.

Let n be an odd prime. Let k be a field with $\operatorname{char} k = p$. Let $G \leq \mathrm{GL}_n(k) = \mathrm{GL}(V)$ be irreducible and finite. If G is not absolutely irreducible, then G must be cyclic and any generator has distinct eigenvalues on V (and is semisimple). So assume that G is absolutely irreducible and k is algebraically closed.

Lemma 5.1. *If $p \neq n$ and the Sylow n-subgroup is not abelian, then G contains a subgroup A of order n such that V is a free kA-module.*

Proof. Let N be a minimal nonabelian n-subgroup of G. Then N acts irreducibly and is extraspecial, whence the result is clear. □

Lemma 5.2. *Suppose that G acts imprimitively.*

(a) *If $n = p$, then the Sylow n-subgroup S of G has order n and V is a free kS-module.*
(b) *If $n \neq p$, then there exists an element $x \in S$ with order a power of n having all eigenspaces of dimension at most* 1.

Proof. Since n is prime, G imprimitive implies that G permutes n one dimensional (linearly independent) subspaces. Thus, G surjects onto a transitive permutation group of degree n. In particular, n divides the order of G. Let N be the normal subgroup of G stabilizing each of the n one dimensional spaces. If $p = n$, then N has order prime to p, whence S has order n and the result follows.

So assume that $p \neq n$. Let $x \in G$ be an n-element with x not in N. Then x^n is central in $\mathrm{GL}(V)$ and its minimal polynomial is $x^n - a$ for some $a \in k^{\times}$, whence the result. □

Note that since n is prime if N is a minimal normal noncentral subgroup of G, then either N is an elementary abelian r-group for some prime $r \neq p$ or N acts irreducibly.

If N acts irreducibly, then either N is an n-group and $p \neq n$, whence N contains a (semisimple) element with distinct eigenvalues or N is quasi-simple. If $Z(N) \neq 1$, then N contains a semsimple element x with $C_V(x) = 0$. If N is simple, then Corollary 1.9 implies that there exists $x \in N$ semisimple with $\dim C_V(x) \leq (1/3)\dim V$ (if $N = \mathfrak{A}_5$, the result follows by inspection).

If N is abelian and not a 2-group, then [12, Cor. 1.3] implies that there exists a (semisimple) $x \in N$ with $\dim C_V(x) < (1/3)\dim V$. Finally, if N is a 2-group and 2 is a multiplicative generator modulo n, then $|N| = 2^{n-1}$ (because G permutes transitively the n eigenspaces of N and the smallest irreducible module of a cyclic group of order n in characteristic 2 has size 2^{n-1}). It follows that there exists $x \in N$ with $-x$ a reflection, whence $\dim C_V(x) = 1 \leq (1/3)\dim V$.

In particular, we have proved part (d) of Theorem 1.5.

We next consider quasi-simple groups and first show:

Theorem 5.3. *Let G be a finite quasi-simple group of Lie type in characteristic p. Let k be an algebraically closed field of characteristic p. Suppose that V is a faithful irreducible kG-module of odd prime dimension $n \leq p$. Then V is a twist of a restricted module and one of the following holds:*

(1) $G = \mathrm{SL}_2(q)$*;*
(2) $G = G_2(q)$ *or* ${}^2G_2(q)'$, $n = 7$*;*
(3) $G = \Omega_n(q)$ *and V is a Frobenius twist of the natural module; or*
(4) $G = \mathrm{SL}_n(q)$ *or* $\mathrm{SU}_n(q)$ *and V is a Frobenius twist of the natural module or its dual.*

Moreover, either there exists a semisimple element $x \in G$ with all eigenspaces of dimension at most 1 *on V or $G = \mathrm{SL}_2(p)$ and $p \leq 2n - 3$. In all cases, there exists a semisimple element $x \in G$ with* $\dim C_V(x) \leq 1$.

Proof. For the first part, it suffices to prove the result for algebraic groups. Let $V = L(\lambda)$ where λ is the highest weight for V. By the Steinberg tensor product theorem and the fact that n is prime, V is a Frobenius twist of some restricted irreducible. So we may assume that λ is p-restricted. By [14], it follows that $L(\lambda)$ is also the Weyl module whence the Weyl dimension formula holds for $L(\lambda)$. Thus, it suffices to work in characteristic 0. The result in that case is due to Gabber, see [15, 1.6].

Aside from the first case, any regular semisimple element of sufficiently large order will have n distinct eigenvalues on V. Suppose that $G = \mathrm{SL}_2(q)$. Let $x \in G$ have order $q+1$. If two distinct weights for a restricted module can coincide on x, then $2\dim V - 2 \geq q+1$. This can only occur if $q = p \leq 2n-3$. Moreover, no nontrivial weight vanishes on an element of order $q+1$. Since a restricted irreducible $k\mathrm{SL}_2(q)$-module has distinct weights, the result follows. □

Theorem 5.4. *Let n be an odd prime. Let $G \leq \mathrm{GL}(V) = \mathrm{GL}_n(k)$ be a finite irreducible quasi-simple group, where k is an algebraically closed field of characteristic p.*

(a) *If $p > \max\{2n-3, n+2\}$ or $p = 0$, then there exists a semisimple $x \in G$ with all eigenvalues distinct.*
(b) *If $p > n+2$, there exists a semisimple element $x \in G$ with $\dim C_V(x) \leq 1$.*

Proof. If p divides $|G|$, then by [8, Thm. B], G is a finite group of Lie type in characteristic p (or $G = J_1, p = 11$ and $n = 7$, where we may take x of order 19) and Theorem 5.3 applies.

If p does not divide $|G|$, then either $p = 0$ or V is the reduction of a characteristic 0 module. The list of possible groups and modules is given in [3, Thm. 1.2]. It is straightforward to see that the conclusion holds for these groups (most of the examples are related to Weil representations). □

Theorem 1.6 now follows from the previous results aside from the case $n = 3$ and $\mathrm{char}\, k = 5$. In that case, any noncentral semisimple element of order greater than 2 has distinct eigenvalues. The next example shows that we do need some restriction on the characteristic.

Example 5.5. Let k be an algebraically closed field of positive characteristic p. Let $G = \mathrm{SL}_p(k) = \mathrm{SL}(V)$. Then G acts by conjugation on $W := \mathrm{End}(V)$. Since every semisimple $g \in G$ is centralized by a maximal torus, we see that $\dim C_W(g) \geq p$. Note that W is a uniserial module with two trivial composition factors and an irreducible composition factor V of dimension $p^2 - 2$. Clearly, $\dim C_V(g) \geq \dim C_W(g) - 2 \geq p - 2$ for any semisimple element g of G (and since semisimple elements are Zariski dense, this is true for any $g \in G$). Note that $\dim V$ can be prime (eg, this is true for $p = 5, 7, 13$). The same holds for $G(p^a) := \mathrm{SL}_p(p^a)$ for any $a \geq 1$.

6. Characteristic Polynomials of Representations

Let G be a group and V a finite dimensional kG-module with k a field of characteristic $p \geq 0$. Let ch_V denote the function from G to $k[x]$ defined by $\mathrm{ch}_V(g) = \det(xI - g)$. Note that two modules have the same function if and only if their composition factors are the same. Our results on bounds for $\dim C_V(g)$ for some $g \in G$ can be phrased in asking: given a kG-module V what is the largest power of ch_k that divides ch_V?

Frank Calegari asked what one could say if V and W are two irreducible kG-modules and ch_V divides ch_W. Calegari and Gee [2] used this information to study Galois representations in very small dimensions.

While we suspect that this does impose some constraints on the representations, we give some examples to show that it is not that rare (at least for groups of Lie type and algebraic groups in the natural characteristic).

Example 6.1. Let G be a simple algebraic group over an algebraically closed field of characteristic $p > 0$. Let V be an irreducible kG-module. By Steinberg's tensor product theorem, $V = V_0 \otimes \cdots \otimes V_m$ where V_i is a twist of a restricted module by the ith power of Frobenius. If 0 is a weight for some V_j, then clearly ch_V is a multiple of $\mathrm{ch}_{V_j'}$, where V_j' is the tensor product of all the $V_i, i \neq j$.

The following example was shown to us by N. Wallach (in particular see [19]).

Example 6.2. Let k be an algebraically closed field of characteristic 0. Let G be a simple algebraic group over k. Let λ and μ be dominant weights with μ in the root lattice. Then $\mathrm{ch}_{V(\lambda)}$ divides $\mathrm{ch}_{V(\lambda+\mu)}$.

It follows the same is true in positive characteristic p as long as p is sufficiently large (depending upon λ and μ). Here are a few cases where one can compute this directly. We give one such case.

Example 6.3. Let k be an algebraically closed field of characteristic $p \geq 0$. Let $G = \mathrm{SL}_n(k)$ and let $V = V(\lambda_1)$ be the natural module. Then $\mathrm{ch}_{V((s+n)\lambda_1)}$ is a multiple of $\mathrm{ch}_{V(s\lambda_1)}$ for $p > s + n$ (or $p = 0$).

References

[1] E. Bertram, Even permutations as a product of two conjugate cycles. J. Combinatorial Theory Ser. A **12** (1972), 368–380.

[2] F. Calegari, T. Gee, Irreducibility of automorphic Galois representations of GL(n), n at most 5. Preprint.

[3] J. Dixon, A. Zalesskii, Finite primitive linear groups of prime degree. J. London Math. Soc. (2) **57** (1998), 126–134.

[4] B. Fein, W. Kantor, M. Schacher, Relative Brauer groups. II. J. Reine Angew. Math. **328** (1981), 39–57.

[5] Y. Fuertes, G. González-Diez, On Beauville structures on the groups S_n and A_n. Math. Z. **264** (2010), 959–968.

[6] R. Gow, Commutators in finite simple groups of Lie type. Bull. London Math. Soc. **32** (2000), 311–315.

[7] R. Guralnick, Some applications of subgroup structure to probabilistic generation and covers of curves. Pp. 301–320 in: *Algebraic groups and their representations* (Cambridge, 1997), NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 517, Kluwer Acad. Publ., Dordrecht, 1998.

[8] R. Guralnick, Small representations are completely reducible. J. Algebra **220** (1999), 531–541.

[9] R. Guralnick, M. Larsen, C. Manack, Low degree representations of simple Lie groups. Proc. Amer. Math. Soc., to appear.

[10] R. Guralnick, G. Malle, Products of conjugacy classes and fixed point spaces. J. Amer. Math. Soc. **25** (2012), 77–121.

[11] R. Guralnick, G. Malle, Simple groups admit Beauville structures. J. London Math. Soc., to appear.

[12] R. Guralnick, A. Maróti, Average dimension of fixed point spaces with applications. Advances Math. **226** (2011), 298–308.

[13] G. Hiss, G. Malle, Low-dimensional representations of quasi-simple groups. LMS J. Comput. Math. **4** (2001), 22–63; Corrigenda: ibid. **5** (2002), 95–126.

[14] J. Jantzen, Low-dimensional representations of reductive groups are semisimple. Pp. 255–266 in: *Algebraic groups and Lie groups*, Austral. Math. Soc. Lect. Ser., 9, Cambridge Univ. Press, Cambridge, 1997.

[15] N. Katz, *Exponential sums and differential equations*. Annals of Math. Studies 124, Princeton U. Press, Princeton, New Jersey, 1999.

[16] P. Kleidman, The maximal subgroups of the finite 8-dimensional orthogonal groups $P\Omega_8^+(q)$ and of their automorphism groups. J. Algebra **110** (1987), 173–242.

[17] F. Lübeck, Small degree representations of finite Chevalley groups in defining characteristic. LMS J. Comput. Math **4** (2001), 135–169.

[18] L. Scott, Matrices and cohomology. Ann. of Math. **105** (1977), 473–492.

[19] N. Wallach, Induced representations of Lie algebras. II. Proc. Amer. Math. Soc. **21** (1969), 161–166.

[20] H. Wielandt, *Finite permutation groups*. Academic Press, New York–London, 1964.

3620 S. Vermont Ave, Department of Mathematics, University of Southern California, Los Angeles, CA 90089-2532, USA.

E-mail address: guralnic@usc.edu

FB Mathematik, TU Kaiserslautern, Postfach 3049, 67653 Kaiserslautern, Germany.

E-mail address: malle@mathematik.uni-kl.de